Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Original) A system for distributing a cryptographic key for encrypting digital data, the system comprising:

a key source for storing the cryptographic key, encrypting the cryptographic key, and for transmitting the encrypted cryptographic key over a control bus; and

a transmitter for receiving the digital data, receiving the encrypted cryptographic key over the control bus, decrypting the encrypted cryptographic key to recover the cryptographic key, encrypting the digital data using the cryptographic key to generate encrypted data, and for transmitting the encrypted data.

2. (Original) The system for distributing a cryptographic key according to claim 1, wherein the key source comprises a first memory for storing the cryptographic key, a second memory for storing an encryption key, and a key encryptor for encrypting the cryptographic key using the encryption key.

3. (Original) The system for distributing a cryptographic key according to claim 1, wherein the transmitter comprises a memory for storing a decryption key, a key decryptor for decrypting the encrypted cryptographic key using the decryption key, and a data encryptor for encrypting the digital data using the cryptographic key.

4. (Original) The system for distributing a cryptographic key according to claim 1, wherein the key source and the transmitter are included in at least two physically separate devices.

5. (Original) The system for distributing a cryptographic key according to claim 1, wherein the control bus is an I^2C control bus.

6. (Original) The system for distributing a cryptographic key according to claim 1, wherein the cryptographic key is encrypted and decrypted using a symmetric system where the encryption key is identical to the decryption key.

7. (Original) The system for distributing a cryptographic key according to claim 6, wherein the symmetric system is a Data Encryption Standard (DES) system.

8. (Original) The system for distributing a cryptographic key according to claim 1, wherein the cryptographic key is encrypted and decrypted using a public key system where the encryption key is public and the decryption key is private.

9. (Original) The system for distributing a cryptographic key according to claim 8, wherein the public key system is a RSA system.

10. (Original) The system for distributing a cryptographic key according to claim 1, wherein the digital data comprises multimedia data, video, audio, web content, graphics or text.

11. (Original) The system for distributing a cryptographic key according to claim 1, wherein the key source is a computer system comprising a first memory for storing the cryptographic key, a second memory for storing an encryption key, a key encryptor for encrypting the cryptographic key using the encryption key, and a microprocessor working together with the key encryptor to encrypt the cryptographic key.

12. (Original) The system for distributing a cryptographic key according to claim 11, wherein the key encryptor is implemented as software running on the microprocessor.

13. (Original) The system for distributing a cryptographic key according to claim 11, wherein the key encryptor is implemented using a firmware or a hardware.

14. (Original) The system for distributing a cryptographic key according to claim 1, wherein the key source and the transmitter are included in a computer.

15. (Original) The system for distributing a cryptographic key according to claim 1, wherein the key source and the transmitter are included in a set-top box.

16 - 22 (Canceled)

23. (Currently Amended) A Digital Video Interface (DVI) system for distributing a cryptographic key for decrypting encrypted data, the system comprising:

a key source for storing the cryptographic key, encrypting the cryptographic key, and for transmitting the encrypted cryptographic key over an I^2C control bus; and

a digital receiver for receiving the encrypted data in DVI format, receiving the encrypted cryptographic key over the I^2C control bus, decrypting the encrypted cryptographic key to recover the cryptographic key, decrypting the encrypted data using the cryptographic key to generate digital data, and for transmitting the digital data in DVI format.

24. (Original) The system for distributing a cryptographic key according to claim 23, wherein the key source comprises a first memory for storing the cryptographic key, a second memory for storing an encryption key, and a key encryptor for encrypting the cryptographic key using the encryption key.

25. (Original) The system for distributing a cryptographic key according to claim 23, wherein the receiver comprises a memory for storing a decryption key, a key decryptor for decrypting the encrypted cryptographic key using the decryption key, and a data decryptor for decrypting the encrypted data using the cryptographic key.

26. (Original) The system for distributing a cryptographic key according to claim 23, wherein receiver is included in a digital display, and the key source is included in a set-top box, a DVD player or a computer.

27-29 (Canceled)

30. (Original) A method of distributing a cryptographic key for encrypting digital data, the method comprising the steps of:

storing the cryptographic key in a key source;

encrypting the cryptographic key in the key source to generate an encrypted cryptographic key;

transmitting the encrypted cryptographic key from the key source over a control bus;

loading the encrypted cryptographic key into a transmitter from the control bus;

decrypting the encrypted cryptographic key in the transmitter to recover the cryptographic key;

introducing the digital data into the transmitter;

encrypting the digital data using the recovered cryptographic key to generate encrypted data; and

transmitting the encrypted data from the transmitter.

31. (Original) The method of distributing a cryptographic key according to claim 30, wherein the key source and the transmitter are included in at least two physically separate devices.

32. (Original) The method of distributing a cryptographic key according to claim 30, wherein both the key source and the transmitter are included in a computer, set-top box, or a DVD player.

33 - 36 (Canceled)

37. (Currently Amended) A method of distributing a cryptographic key for decrypting encrypted data in Digital Video Interface (DVI) format, the method comprising the steps of:

storing the cryptographic key in a key source;

encrypting the cryptographic key in the key source to generate an encrypted cryptographic key;

transmitting the encrypted cryptographic key from the key source over an I^2C control bus;

loading the encrypted cryptographic key into a digital receiver from the I^2C control bus;

decrypting the encrypted cryptographic key in the digital receiver to recover the cryptographic key;

introducing the encrypted data in DVI format into the receiver;

decrypting the encrypted data using the recovered cryptographic key to generate decrypted data; and

transmitting the decrypted data from the digital receiver.

38. (Original) The method according to claim 37, wherein the receiver is included in a digital display, and the key source is included in a set-top box, a DVD player or a computer.

39 - 40. (Canceled)

41. (New) A Digital Video Interface (DVI) system for distributing a cryptographic key for encrypting digital data, the system comprising:

a key source for storing the cryptographic key, encrypting the cryptographic key, and for transmitting the encrypted cryptographic key over an I^2C control bus; and

a digital transmitter for receiving the digital data in DVI format, receiving the encrypted cryptographic key over the I^2C control bus, decrypting the encrypted cryptographic key to recover the cryptographic key, encrypting the digital data using the cryptographic key to generate encrypted data, and for transmitting the encrypted data in DVI format.

42. (New) A Digital Video Interface (DVI) system for distributing a cryptographic key for decrypting encrypted digital data, the system comprising:

a key source for storing the cryptographic key, encrypting the cryptographic key, and for transmitting the encrypted cryptographic key over an I^2C control bus; and

a digital receiver for receiving the encrypted data in DVI format, receiving the encrypted cryptographic key over the I^2C control bus, decrypting the encrypted cryptographic key to recover the cryptographic key, decrypting the encrypted data using the cryptographic key to generate digital data, and for displaying an image corresponding to the digital data.

43. (New) A method of distributing a cryptographic key for encrypting digital data in a Digital Video Interface (DVI) system, the method comprising the steps of:

storing the cryptographic key in a key source;

encrypting the cryptographic key in the key source to generate an encrypted cryptographic key;

transmitting the encrypted cryptographic key from the key source over an I^2C control bus;

loading the encrypted cryptographic key into a digital transmitter from the I^2C control bus;

decrypting the encrypted cryptographic key in the digital transmitter to recover the cryptographic key;

introducing the digital data into the digital transmitter;

encrypting the digital data using the recovered cryptographic key to generate encrypted data in DVI format; and

transmitting the encrypted data from the digital transmitter.

44. (New) A method of distributing a cryptographic key for decrypting encrypted data in Digital Video Interface (DVI) format, the method comprising the steps of:

storing the cryptographic key in a key source;

encrypting the cryptographic key in the key source to generate an encrypted cryptographic key;

transmitting the encrypted cryptographic key from the key source over an I^2C control bus;

loading the encrypted cryptographic key into a digital receiver from the I^2C control bus;

decrypting the encrypted cryptographic key in the digital receiver to recover the cryptographic key;

introducing the encrypted data into the receiver in DVI format;

decrypting the encrypted data using the recovered cryptographic key to generate decrypted data; and

displaying an image corresponding to the decrypted data on a digital display.